



06

## Autorizando el acceso

### Transcripción

[00:00] Hola a todos y todas, bienvenidos y bienvenidas a este nuevo video sobre Servlet. En el video pasado vimos el sobre nuestro código, que evitaba que una persona que no estaba logueada pueda entrar en listaEmpresas.

[00:17] Y vimos que no era una buena idea por ejemplo copiar este código y pegarlo en cada uno de las otras acciones, para evitar que la persona entre las otras acciones cuando no está logueado, ya que sería un "Ctrl + C", "Ctrl + V" en cada uno de ellos, y eso es una mala práctica, porque si en el futuro decidimos cambiar esta regla y decir: "no, no va a llamarse loginUsuario, va a llamarse login, no sé", tendríamos que cambiarlo en cada uno de esos archivos.

[00:53] Entonces no es buena idea tener ese mismo código repetido en muchos lugares. Es mejor tenerlo en un lugar único y como un lugar único, una buena idea sería colocarlo tal vez en entrada, en nuestro servlet, nuestro controlador, entonces vamos a cortar este código, cortar. "Ctrl + Shift + O" para sacar ese input que está ahí y vamos a ponerlo por acá arriba.

[01:16] Vamos a colocar acá arriba. Y nos está dando un problema, un error. Nos está diciendo que no podemos usar ese return. Tenemos que usar nuestro response.sendRedirect. Voy a copiar y voy a pegar esto de acá y en vez de hacer sendRedirect ahí va a tener que ir a nuestro LoginForm, tiene que ir a nuestro LoginForm. Voy a sacar toda esta parte de acá para no confundir.

[01:52] Entonces, si nuestro usuario no está logueado, entonces tiene que ir a nuestro LoginForm. Voy a sacar esto de acá, que es un poco confuso y vamos

colocar eso en una variable. Vamos a colocar Boolean `esUnUsuarioLogado` = es igual a esto. Entre paréntesis, bien y acá vamos a colocar `If esUnUsuarioLogado`.

[02:32] Sería un usuario no logado, `esUnUsuarioNoLogado`. Ahí está. Coloque una O mayúscula, ahí está. O minúscula. Bien, si no es un usuario logado entonces lo reenvío al login. Vamos a ver qué es lo que ocurre. "Ctrl + S", voy a hacer un "Ctrl + S" acá, bien y vamos a ir a nuestra `listaEmpresas`, `listaEmpresas` y nos está dando un error. ¿Qué es lo que nos está dando?

[03:07] Vean que es un 500, un error del servidor, vamos a tener más información si nosotros vemos en el stack trace de nuestro servidor. Dejen que voy a colocar de nuevo la vista del servidor. Acá tenemos nuestro servidor y tenemos la consola, doble clic en la consola para expandir esto.

[03:34] Dice: "No puedo reenviar después de que la respuesta se haya llevado a cabo". Un mensaje un poco extraño, ¿pero qué es lo que ocurre en realidad? Nosotros tenemos un response, nosotros estamos respondiendo a nuestro navegador, le estamos diciendo: "hacé un redirect a nuestro login". ¿Pero qué es lo que ocurre?

[03:51] Después de esto el código sigue ejecutándose, tenemos más código acá. Y acá nosotros estamos enviando otro response, entonces no deberíamos continuar ejecutando si ya hemos hecho un redireccionamiento. Entonces lo que podemos hacer es colocar acá un `return`. con eso nosotros evitamos que se siga ejecutando el resto del código.

[04:14] Bien, vamos a ver qué es lo que está ocurriendo. "Ctrl + S", el servidor se va a reiniciar. Y vamos a ver `listaEmpresas`. Enter. Nos está diciendo `LoginForm` no está siendo encontrado, ¿por qué? Porque me faltó colocar acá que es "entrada?accion=LoginForm". Creo que es eso lo que me ha faltado, restart.

[04:49] A ver, gerenciador/entrada?ListaEmpresas, enter. Nos está dando otro error. Acá dice: Error too many redirects. Ven que me redireccionó al LoginForm, entonces eso está bien. Yo puse acá listaEmpresas, pero ahora me reenvió a LoginForm, y acá me está diciendo: hay muchos redirects. ¿Qué es lo que está ocurriendo?

[05:15] Cuando un usuario no está logueado yo lo reenvío a nuestra acción de LoginForm. Para entrar en nuestra acción de LoginForm tiene que entrar de nuevo en este controlador. Y en este controlador estoy preguntando si el usuario no está logueado.

[05:33] Pero es una cosa extraña porque el LoginForm sirve para que la persona pueda loguearse, o sea, no está logueada y se va a bloquear. Entonces, esta acción de acá no debería ejecutarse para ese LoginForm, ni para ese LoginForm ni para el login, para todas las demás, eliminarEmpresas, listarEmpresas, modificar, mostrar nuevaEmpresa, todas esas deberían pasar por esta regla, pero no nuestro LoginForm y nuestro login.

[06:02] Entonces. Vamos a ver eso. ¿Cómo hacemos para saber cuál es la acción a la que estamos intentando entrar? Tenemos esta línea acá, que obtenemos nuestra acción, entonces vamos a llevar esa línea para arriba, vamos a llevarla acá. Bien, acá tenemos nuestro paramAccion.

[06:26] Ahora tenemos que preguntar lo siguiente. Antes de continuar, déjenme ordenar un poco el código, voy a colocar las variables acá. Esta otra variable que hemos creado nosotros acá para ver si es un usuario logado, lo dejamos ahí y lo que me gustaría saber es si esta acción es listaEmpresas.

[06:47] Entonces Boolean, vamos a ver, esUnaAcciónProtegida, voy a crear esa variable que sirve para identificar cuáles son las acciones que están protegidas, es decir, las acciones que no pueden una persona entrar sin haberse logueado antes, que necesitan estar logueadas antes de poder entrar ahí, entonces es igual a vamos a ver si el paramAccion.equals.

[07:22] Vamos a ver si es igual a "ListaEmpresas". Si es igual a eso, entonces, este usuario debería tener que redirigirse, tendría que ir al login, entonces es un si no está logueado y && esUnaAccionProtegida, o sea, si no está logueado e intenta acceder a listaEmpresas, entonces tiene que ir a LoginForm.

[08:01] Vamos a ver si esto está funcionando, "Ctrl + S", se reinicia el servidor y vamos a ver, nuestra acción es listaEmpresas. Funcionó. Nuestra lista de empresas nos redirigió al LoginForm y no fue hecha muchas veces esa redirección. Entonces esta parte de acá está funcionando. ¿Cómo hago yo para poder listar todas las acciones que necesitan, o sea, que son protegidas?

[08:39] Nosotros tenemos muchas acciones, tenemos eliminar, modificar, mostrar, son muchas acciones, y en vez de colocar cada una de esas acciones paramAccion equal ListaEmpresas o ese paramAccion equals mostrarEmpresa, etcétera, vamos a hacer un truco y en vez de colocar solo las acciones que son protegidas, vamos a ver las acciones que no son protegidas, es decir, las acciones que no necesitan que estés logueado para poder entrar, que es login y LoginForm.

[09:13] Solamente tenemos dos acciones que no son protegidas, entonces es más fácil colocar esa lista de acciones que la otra lista de acciones protegidas. Entonces vamos a hacer un truco. Vamos a hacer lo siguiente.

[09:27] Vamos a ver, voy a colocar un paréntesis acá y en vez de colocar las acciones "ListaEmpresa", voy a colocar la acción ("Login"), esa o si la acción a la que estoy intentando acceder es equals("LoginForm"), si es cualquiera de esas acciones, perdón, si no es, acá estoy negando, si no es login ni LoginForm, entonces significa que es una acción protegida.

[10:07] Es una acción protegida. Entonces siesta lógica está correcta, con "Ctrl + S" vamos a probar a ver si esto está funcionando. Vamos a ver, vamos a ir a eliminarEmpresa, perdón, eliminarEmpresa no. ListaEmpresas. Bien, nos

redirigió el login, vamos a probar con eliminarEmpresa con id cualquiera, nos está redirigiendo al login.

[10:36] Si yo intento ir al login, perfecto. No hay problema. ¿Qué pasa si coloco mi usuario y mi contraseña? 12345. Enviar, conseguí hacer un login, conseguí ir a listarEmpresas. Vamos a ver el modificar, modificar también funciona. ¿Por qué? Porque ya me logueé, entonces ya nuestra sesión ya guardó ese session id con ese usuario y ya estoy pudiendo acceder a todas las acciones siempre y cuando me haya logueado anteriormente.

[11:15] Vamos a probar acá una última vez con un navegador incógnito localhost, acción listaEmpresas, me redirige a nuestro Login. Entonces esto está funcionando. Bien. Ahora una cosa que no me gusta tanto, este código de acá nosotros lo hemos colocado en el controlador y podemos decir bueno, es lógico ponerlo ahí, ya que estamos controlando el acceso, la autorización de las personas a ciertas acciones.

[11:49] Entonces es lógico ponerlo ahí, en el controlador. Pero imaginen lo siguiente, si nosotros usamos un framework como sprint MVC, ¿vamos a reescribir el controlador de sprint solo para colocar ese código nuestro de autorización? O sea, tendríamos que modificar el controlador de la persona que escribió ese controlador de sprint, recompilarlo y usarlo.

[12:20] Es un poco raro hacer eso, no sería realmente algo una buena opción. Entonces lo que vamos a ver en el próximo video es dónde colocar este código sin ser acá en el controlador y que aun así podamos utilizarlo como como puerta de autorización para nuestros forms, perdón, para nuestras acciones. Entonces vamos a ver eso en el próximo video.